WHITE PAPER

Mastering Cloud Security: Navigating Today's Threat Landscape

Contents

Introduction

It is the morning of July 19, 2024. Across the globe, IT professionals rest peacefully, having deployed a wealth of sophisticated technologies to protect their applications and data, hosted in tens of thousands of cloud resources.

For it's a dangerous world out there on the open internet. Viruses, worms, phishing, ransomware, advanced persistent threats (APTs), emanating from bad actors ranging from scammers and con artists to organized crime and hostile nation-states.

Those security experts know: it's a race to deploy the best defenses against the latest threats as quickly as possible.

Every application, every database, every network, is supported by antivirus, multi-factor authentication, end-to-end encryption, cloud access security brokers, firewalls, gateways, AI-intrusion detection systems, incident response processes… the list goes on.

Then all hell breaks loose.

"I am convinced that there are only two types of companies: those that have been hacked and those that **will be**."

Robert S. Mueller III
Director, United States Federal Bureau of Investigation, at **RSA 2012**

The Second Decade of the Cloud Brings New Security Challenges

We are now midway through the second decade of cloud computing. Enterprises have found that the cloud has largely fulfilled its promise: IT organizations have cut infrastructure and operations costs, closed data centers, and have taken advantage of the unique capabilities of the cloud: elastic scale, container-based and serverless applications, and, of course, AI. Indeed, in EPAM's recent **Cloud Mastery survey**, 77% of respondents said that not just IT change but business transformation was a key benefit of cloud computing.

However, there is a darker side: security incidents in the cloud are doubling every year, according to Verizon's **Data Breach Investigations Report** (DBIR). CISOs and CIOs must be aware of and take action against the growing and evolving threats.

The stakes are very, very high. So serious, in fact, that the **World Economic Forum** — noting that the financial services sector has lost $12 billion from cyberattacks in the past twenty years (rising consistently year over year) — recently warned that "global financial stability is at risk due to cyber threats."

And, as per **Gartner®**, "By 2028, 25% of enterprise breaches will be traced back to AI agent abuse, from both external and malicious internal actors."[1]

It's vital that CIOs and CISOs adapt and respond to the demands of security in the cloud. Here, we present an overview of the emerging challenges and five key guidelines critical to your organization's secure journey to Cloud Mastery.

As the Threat Landscape Evolves, So Must Security Teams

As the complexity of enterprise software has grown over the past few decades, so has the sophistication of the threats facing it; developers and IT professionals scramble to maintain their defenses against attacks that could come from anywhere at any time.

A few decades ago, so-called "script kiddies" created unsophisticated viruses and worms (like the famous "**ILOVEYOU**" virus) that wreaked havoc only because operating systems were utterly unprepared for them.

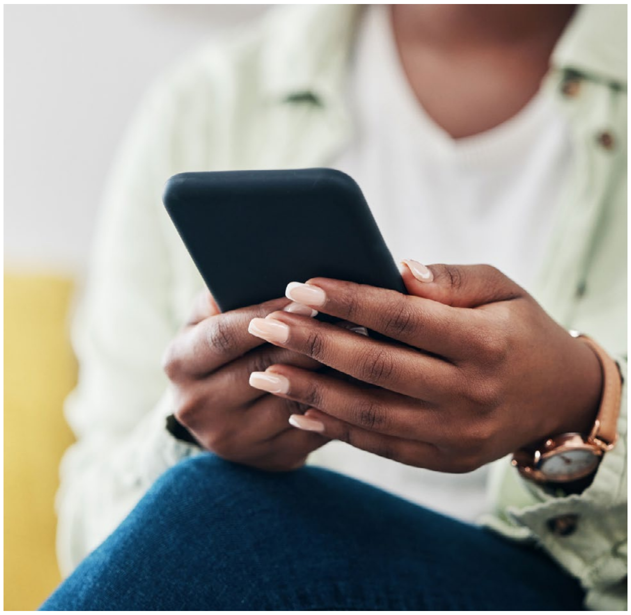
> "Cybercrime to Cost the World $10.5 Trillion Annually [in] 2025."
>
> **Cybersecurity Ventures**

[1] Gartner, Predicts 2025: AI's Impact on the Future of Enterprise Technology, Arun Chandrasekaran et. Al. 18 March 2025

Today, however, organized crime and nation-states pour vast resources into understanding the deep internals of computer systems to find vulnerabilities — to steal secrets, money or otherwise manipulate people and decisions. And companies increasingly need to protect against not only external hackers, but also from malfeasance (intentional or accidental) by insiders — employees, contractors, and anyone with access to the network.

Worse, because of the increasing complexity of these systems, misconfigurations due to human error are easy and are the most common cause of breaches. Customer misconfigurations of Amazon Web Services' S3 storage buckets may account for almost **20% of cloud breaches**. Even the most advanced technology vendors are not immune: because of a misconfigured server on **Microsoft's own network**, hackers were able to gain access to confidential business data.

And worst of all, as the world discovered last July, even the software intended to protect our systems can, because of a simple human error, cause catastrophic outages. The security vendor **CrowdStrike** delivered a faulty update — and tens of thousands of Windows servers would no longer reboot. This outage caused global disruption; cancelled flights left airline passengers stranded and hospital mission-critical systems went dark. As the largest outage in history, the faulty update cost CrowdStrike customers tens of billions of dollars; Fortune 500 companies alone estimated some **$5.4 billion in direct losses**.



The New Attack Vector: AI

As organizations enter 2025, they face new kinds of attacks based on generative AI (GenAI). GenAI offers enterprises an incredible array of benefits, but with it comes new threats that security professionals must guard against. Users can inadvertently feed confidential information to public models; internal models can be "poisoned," that is, fed bad or malicious training data to give incorrect results; and malicious users can use GenAI to "socially engineer" hacks to more effectively personalize phishing campaigns, impersonate employees and even use realistic deepfakes to fool security safeguards.

Do the Cloud Vendors "Handle Security" for You?

As organizations now rely primarily on the cloud, a common misconception remains that cloud vendors — Microsoft, Amazon, Google — "take care of security." Nothing could be further from the truth. In fact, security professionals today embrace the notion of a shared responsibility model, meaning that while the vendors do indeed guarantee the security of the infrastructure (physical security, hardware, core software), organizations must take the appropriate steps to secure their applications, identities and data.

That means that the job of CISOs and their teams has, if anything, become more demanding. They must:

- Protect enterprise data from unauthorized access and exfiltration
- Protect their employees from unauthorized or unacceptable behavior both from within the enterprise and from outside it
- Protect applications from viruses, malware and intrusion

As attackers have become more sophisticated, so too have the tools; and these require that IT professionals know how to take advantage of them.

The Network is Flat

In 2005, New York Times columnist Tom Friedman wrote ***The World Is Flat***; the book's thesis was that technology has, in effect, removed many of the barriers between nations and peoples.

The title serves as a useful analogy for the revolutionary changes we have seen in computing over the past few decades. Think about it: When enterprises managed their own data centers, their own servers, storage, hops and routers, enterprise networks were nothing if not complex. Subnets, active directory domains and forests, DMZs, firewalls and yes, routers: all these things made managing networks difficult (how many of us remember debugging router loops?) … but also made it difficult for those trying to break in. Perhaps a hacker could get into one segment of a corporate network, but be blocked from another, simply because of how IT had connected it.

But in the cloud, everything is connected to everything: a flat network model. The relatively smaller number of hops makes a lateral attack easier — meaning that their attacks can spread once hackers gain access through any entry point. Once you're in, you're in. The blast radius is huge, and lets bad actors remain undetected in the network often for weeks before detection.

Most organizations have dealt with this through micro-segmentation: by deploying a host of defenses, ranging from firewalls and bastions to virtual networks and application gateways. While these services are powerful, they come with complexity and overhead. You must configure them, set up alerts and monitor them either by humans or through other real-time analytics systems, and so on.

Moreover, it's often difficult to know just how much technology is enough. Does your firewall need packet inspection features? Do you need Layer 7 Distributed Denial of Service (DDOS) protection? How much protection is needed at the endpoint to protect against viruses or spearphishing?

And, as our survey noted, most customers use more than one public cloud — these gaps between clouds can be dangerous. They must be secured, their authentication models must be harmonized, data flowing across the public internet must be carefully protected. The hackers know that where there's a gap, there's a way in.

In our survey, one result stood out as particularly troubling: most respondents considered security easier in the cloud than on-premises.

That might have been true years ago. Not now.

01

Implement Core Security Hygiene

So, what to do? A good place to start is what we call “core security hygiene.” These are the basics. If the network is “flat,” that is, there are few physical barriers between resources, then a new philosophy is needed. Nothing accessing enterprise resources can be trusted without verification — not users, not other systems.

This approach, called zero trust, leverages various technologies to harden every resource, including:

01

Data Classification According to Sensitivity

Sensitive data must be classified and labeled as such. For example, sensitive IP — the primary target for hackers — should be labeled as “Secret” or “Highly Sensitive;” automated policies should then be used to limit access to authorized personnel or workloads.

02

Enterprise Perimeters

Building and securing the boundaries of the enterprise network in the cloud is made possible thanks to, in AWS terms, a virtual private cloud (VPC), or in Microsoft’s, a virtual network (VNet). VNets and VPCs allow organizations to safely deploy and manage resources by creating isolated zones for different security levels.

03

Encryption & Key Management

Today, cloud resources enforce network (in-transit) and storage (at-rest) encryption by default, reducing the possibility of someone “sniffing” network traffic. However, in order to safeguard encryption keys, developers must use key management systems (KMSs) such as Azure Key Vault, AWS Key Management or Google’s Cloud Key Management as the basis for a key management lifecycle: generating keys, rotating them on a periodic basis, revoking them as required, and so on.

For particularly sensitive applications, a new technology (mentioned above) called confidential computing supports the most advanced use of encryption — in memory, meaning that code and data are only decrypted when they enter the CPU for use.

04

Robust Identity & Access Controls

As the weaknesses of simple password access have become apparent, many are turning to multi-factor authentication (MFA), using phone or email callbacks, biometric verifications or hardware tokens to prevent imposters from accessing the network. Application access using role-based access control (RBAC), which provides access to data based on a pre-defined role. are increasingly adopting the principle of least privilege, which restricts access to only what’s needed to perform a task.

Zero trust is just the beginning — and it’s table stakes for mastering cloud security.

02

Adopt Detection & Response as Defense Strategies

Attacks, attempted intrusions, phishing, ransomware — these happen every day, to every organization. Detecting them and responding appropriately and carefully are essential elements of the CISO's role.

Detection & Observability

As organizations select which cloud services to adopt or build, an important criterion is how observable they are. Can you see if a hacker is trying to break in? For example, if nearly all your logins are coming from the U.S. and Europe, but just a few from, say, Mongolia (and you have no employees there) … well, that's likely an attack.

Logs and alerts are the security professional's friend. The events captured in them — whether recorded in a database or sent via a high-priority text message — can warn of suspicious activity, such as attempts at unauthorized access, data exfiltration or (even) insider trading.

However, the amount of data logging systems collect today is staggering. Security information event management (SIEM) systems rapidly analyze the data, analyze behavior of entities in the logs, and correlate potentially related events, which helps security professionals respond quickly.

Resources such as the U.S. **Cybersecurity and Infrastructure Security Agency** and the UK's **Cyber.uk** regularly publish information about both recently discovered vulnerabilities in software systems and emerging threats; and many SIEM systems connect to such "threat intelligence" sources to improve their analyses.

But know: the bad guys are aware of these resources too and use them. When CISA alerts about a vulnerability, act promptly.

Know How to Respond

Security incidents demand a response. CISOs and their teams should determine and implement the best strategies for handling them. For example, use automated tools to detect and quarantine phishing emails, and possibly blacklist the sender's IP address.

To safeguard against the broader threats of ransomware and other such attacks, ensure you have safe, isolated backups (where ransomware can't access them). Also, consider creating and regularly rehearsing incident recovery plans, with well-defined roles for your security teams, employees and outside agencies such as law enforcement.

03

Train Your Developers

It used to be a common misconception that development teams "added security" as they completed their work. Today, CIOs and CISOs must recognize that security must be a consideration at every phase of the development cycle. They must ensure that their development teams internalize its importance, using **Security by Design**.

Methodologies like Microsoft's Secure Design Lifecycle (SDL) and the Open Web Application Security Project (OWASP) provide guidelines to help developers by insisting they:

Validate all input to verify that data is within range, the right format, the expected data type, and so on.

Analyze potential threats by performing an architectural assessment of the software, examining it for potential weaknesses, and understanding the external threat landscape with open source intelligence (OSINT), logs and industry reports.

Make security part of the build process, ensuring that antivirus software is built in and vulnerability testing is part of the CI/CD pipeline.

Use strong authentication, such as MFA or biometric means to prevent unauthorized access.

Ensure frameworks and libraries used are secure and up-to-date with the latest security updates. An out-of-date open source library caused a massive breach in a credit bureau in 2017; an estimated 200,000 credit card numbers were stolen.

Test extensively with a range of tools such as chaos and penetration testing.

Developing with security in mind isn't easy. Make sure that your development teams receive the proper training before starting to code.

04

Train Everyone Else, Too

According to the 2025 **Phishing Trends Report**, over 60% of businesses reported phishing attacks over email, with an average cost of $150,000 per incident. The report also notes that such attacks — in which fraudulent emails can appear legitimate and valid — target employees in financial positions.

"Around 80% of phishing campaigns aim to steal credentials..."

2025 Phishing Trends Report

These troubling statistics highlight the urgency of employee awareness of the cyberthreats surrounding them. While many companies provide such training through videos and quizzes, life-like rehearsals and roleplay (just like security teams do) can more effectively empower the entire workforce to know what to do when they encounter malicious activity.

Security is not just the InfoSec department's responsibility: **it's everyone's.**

05

Build Strong Governance

A strong cloud security governance function, led and reporting to the CIO and/or CISO, helps ensure that all the technologies and processes that you've mandated are being properly and comprehensively used.

Every organization, sooner or later, will face a potential security violation. The governance body should set the incident response processes executed if a possible breach is detected: which events should trigger such a process, who should be notified, what their playbooks are, how to shut down and/or restore critical systems.

Key responsibilities of the governance organization (or groups responsible to it) include:

Maintaining an up-to-date inventory of all applications and data maintained by the organization; what they do, what they hold, their current security posture and how current they are with security updates.

Ensuring that best practices, such as zero trust and secure development approaches, are followed. This requires quantitative oversight via ongoing reporting. While exceptions may, in extraordinary circumstances, be allowed, they should be reviewed by CxO.

Understanding where sensitive data is stored and ensuring that it is properly protected. For example, only authorized people and applications can access personally identifiable information (PII), while the system anonymizes it for everyone else.

These five principles summarize the basics. But they are not enough, because in November 2022 the world — of applications, of IT, and of security — changed.

AI Changes the Paradigm & Brings New Risks

Since the introduction of ChatGPT, organizations have been racing to incorporate AI into their solutions. It brings new ways to connect with customers, forecast sales, improve marketing and expedite operations… to name a few.

But AI also provides a new toolkit to the hacker community.

AI: New Tools for Hackers

Just as enterprises are learning how to use AI, so are the cybercriminals, who are becoming increasingly knowledgeable and sophisticated about how to use it for their own purposes.

And because AI is such a broad-reaching technology, they can use it in many ways:

01

Model Supply Chain Vulnerabilities

In February 2024, Hugging Face, a collaboration repository holding thousands of downloadable models and datasets, discovered approximately 100 malicious models.

02

Hack Acceleration

In the same way that tools like GitHub Copilot and Cursor.com can be used to help legitimate developers speed coding, they can also be used by hackers with their attack code.

03

Social Engineering & Deepfakes

Without much effort, a model can be trained to both send texts and emails that sound exactly like an employee; and more sophisticated AI engines can be trained to look like a real person and speak in their voice (deepfakes). Seeing a realistic deepfake carrying on a conversation in real-time with an unsuspecting user doesn’t take much imagination.

04

Model Poisoning

Many companies are now training their LLMs and SLMs with their own data for internal use. These models, of course, depend upon the quality of the training data; however, a malicious user could “poison” the model with invalid data to influence investment decisions. Google’s DeepMind AI project, a forerunner of its Gemini LLM, was poisoned in this way in 2023 when malicious actors manipulated training images. Google was quick to address the issue, but not all companies have the resources or expertise to identify, let alone address, such issues.

But AI Benefits CISOs As Well

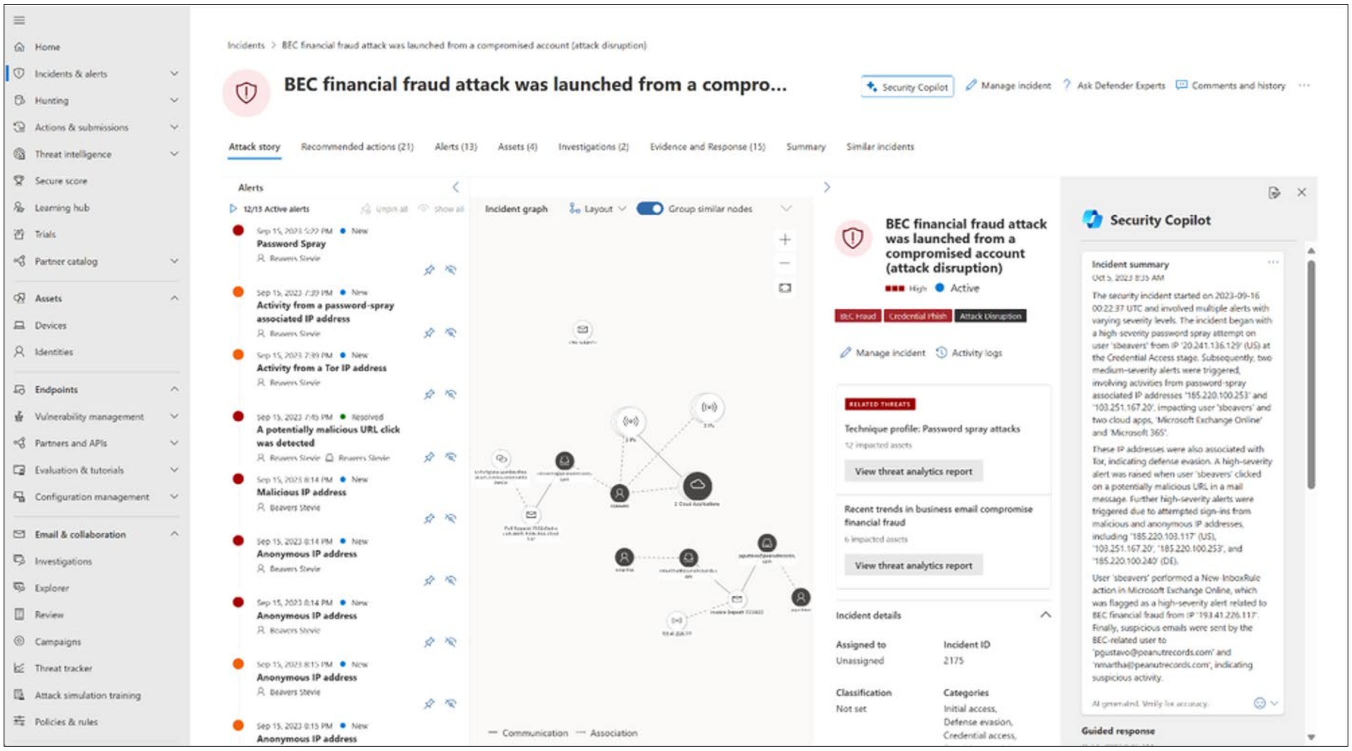
Fortunately, AI can be also used for good and offers important advantages for CISOs and their teams.

Because AI is particularly good at analyzing large volumes of data, it is well suited for discovering issues and patterns within the voluminous event logs generated by security tools. For example, it can easily spot anomalous network and login behaviors or correlate activities with compromised accounts as the example below shows.

Additionally, agentic AI tools can parse and correlate events in real time — and then take coordinated actions on the organization's behalf. For example, an automated security agent may be able to send alerts, isolate affected systems, shut down compromised accounts and so on.

Further, armed with this data and knowledge of the organization's configuration, AI tools can scan devices to look for vulnerabilities and recommend system or application updates. Such tools can also perform predictive analysis on likely threats or attack vectors.

Finally, it is not terribly difficult to imagine that such tools could, in the future, analyze the company's strategies, plans, assets and employee makeup to understand how future threats might unfold.



Incidents > BEC financial fraud attack was launched from a compromised account (attack disruption)

BEC financial fraud attack was launched from a compro...

Alerts

12/13 Active alerts

Sep 15, 2023 5:22 PM • New
Password Spray
Beavers Stevie

Sep 15, 2023 7:39 PM • New
Activity from a password-spray associated IP address
Beavers Stevie

Sep 15, 2023 7:39 PM • New
Activity from a Tor IP address
Beavers Stevie

Sep 15, 2023 7:45 PM • Resolved
A potentially malicious URL click was detected
Beavers Stevie Beavers Stevie

Sep 15, 2023 8:14 PM • New
Malicious IP address
Beavers Stevie

Sep 15, 2023 8:14 PM • New
Anonymous IP address
Beavers Stevie

Sep 15, 2023 8:14 PM • New
Anonymous IP address
Beavers Stevie

Sep 15, 2023 8:15 PM • New
Anonymous IP address
Beavers Stevie

Sep 15, 2023 8:15 PM • New
Anonymous IP address

BEC financial fraud attack was launched from a compromised account (attack disruption)

High • Active

BEC Fraud | Credential Phish | Attack Disruption

Manage incident | Activity logs

RELATED THREATS

Technique profile: Password spray attacks
12 impacted assets
View threat analytics report

Recent trends in business email compromise financial fraud
6 impacted assets
View threat analytics report

Incident details

Assigned to: Unassigned
Incident ID: 2175
Classification: Not set
Categories: Initial access, Defense evasion, Credential access,

Security Copilot

Incident summary
Oct 5, 2023 8:35 AM

The security incident started on 2023-09-16 00:22:37 UTC and involved multiple alerts with varying severity levels. The incident began with a high-severity password spray attempt on user 'sbeavers' from IP '20.241.136.129' (US) at the Credential Access stage. Subsequently, two medium-severity alerts were triggered, involving activities from password-spray associated IP addresses '185.220.100.253' and '103.251.167.20', impacting user 'sbeavers' and two cloud apps, 'Microsoft Exchange Online' and 'Microsoft 365'.

These IP addresses were also associated with Tor, indicating defense evasion. A high-severity alert was raised when user 'sbeavers' clicked on a potentially malicious URL in a mail message. Further high-severity alerts were triggered due to attempted sign-ins from malicious and anonymous IP addresses, including '185.220.103.117' (US), '103.251.167.20', '185.220.100.253', and '185.220.100.240' (DE).

User 'sbeavers' performed a New-InboxRule action in Microsoft Exchange Online, which was flagged as a high-severity alert related to BEC financial fraud from IP '193.41.226.117'. Finally, suspicious emails were sent by the BEC-related user to 'pgustavo@peanutrecords.com' and 'nmartha@peanutrecords.com', indicating suspicious activity.

AI generated. Verify for accuracy.

Guided response

Figure 1 Microsoft Security Copilot (source: **Microsoft**)

Conclusions: Ever Learning, Ever Vigilant

Breaches are always imminent — but you can be ready. In the early days of the cloud, security seemed, perhaps, straightforward. But today, like so many other aspects of cloud computing, is very complex, requiring constant attention, expertise and learning.

In this piece, we've covered aspects of cloud security at a high level, outlining some of the lessons we ourselves have learned by deploying complex solutions for our clients. Probably the most important lesson is that every organization needs trained, experienced experts who can guide their cloud security journey, and their teams and, at the end of the day, leave them in control of their cloud ecosystem.

Cloud security is **essential**:
pay it the attention it deserves.

Resources

Cloud Security Alliance

Cybersecurity and Infrastructure Security Agency

Cyber.uk

Azure Security

AWS Security

Google Cloud Security

CISA

NIST: Preparing for Ransomware

Gartner Report*

*The Gartner Report(s) described herein, (the "Gartner Report(s)") represent(s) data, research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. ("Gartner"), and are not representations of fact. Each Gartner Report speaks as of its original publication date (and not as of the date of this Prospectus) and the opinions expressed in the Gartner Report(s) are subject to change without notice.

About EPAM

Since 1993, EPAM Systems, Inc. (NYSE: EPAM) has used its software engineering expertise to become a leading global provider of digital engineering, cloud and AI-enabled transformation services, and a leading business and experience consulting partner for global enterprises and ambitious startups.

We address our clients' transformation challenges by fusing EPAM Continuum's integrated strategy, experience and technology consulting with our 30+ years of engineering execution to speed our clients' time to market and drive greater value from their innovations and digital investments.

We leverage AI and GenAI to deliver transformative solutions that accelerate our clients' digital innovation and enhance their competitive edge. Through platforms like EPAM AI/RUN™ and initiatives like DIALX Lab, we integrate advanced AI technologies into tailored business strategies, driving significant industry impact and fostering continuous innovation.

We deliver globally, but engage locally with our expert teams of consultants, architects, designers and engineers, making the future real for our clients, our partners and our people around the world.

We believe the right solutions are the ones that improve people's lives and fuel competitive advantage for our clients across diverse industries. Our thinking comes to life in the experiences, products and platforms we design and| bring to market.

Added to the S&P 500 and the Forbes Global 2000 in 2021 and recognized by Glassdoor and Newsweek as Most Loved Workplace, our multidisciplinary teams serve customers across six continents. We are proud to be among the top 15 companies in Information Technology Services in the Fortune 1000 and to be recognized as a leader in the IDC MarketScapes for Worldwide Experience Build Services, Worldwide Experience Design Services and Worldwide Software Engineering Services.

Learn more at **www.epam.com** and follow us on **LinkedIn**.

Headquarters

41 University Drive, Suite 202
Newtown, PA 18940, USA

P: +1-267-759-9000
F: +1-267-759-8989

EPAM.COM